(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2003188873 A

(43) Date of publication of application: 04.07.03

(51) Int. Cl H04L 9/32
G09C 1/00

(21) Application number: 2001380971

(22) Date of filing: 14.12.01

(71) Applicant: KANAZAWA INST OF TECHNOLOGY

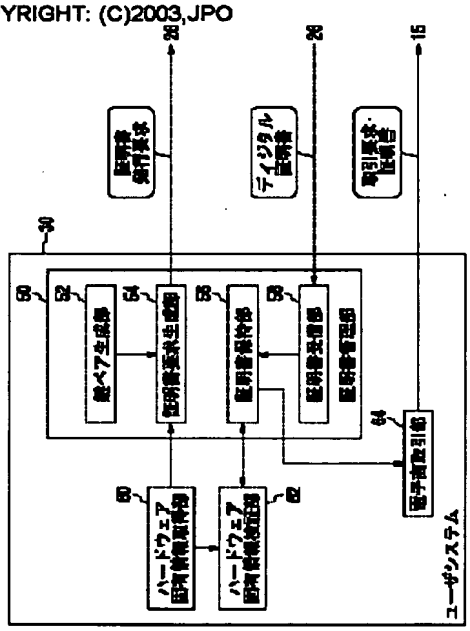
(72) Inventor: HATTORI MICHIMITSU
SENGOKU YASUSHI

(54) AUTHENTICATION METHOD, AUTHENTICATION DEVICE WHICH CAN UTILIZE THE METHOD, USER SYSTEM AND AUTHENTICATION SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent the illegal behavior of a user such as complete faking in e-commerce.

SOLUTION: A hardware characteristics information obtaining part 60 obtains identification information characteristic to hardware utilized by the user. A certificate request generation part 54 transmits the public key of the user generated by a key pair generation part 52 and the characteristic information of the hardware to an authentication device 26 as user information, and a certificate reception part 58 receives a digital certificate having the hardware characteristics information incorporated therein from the authentication device 26 and holds it in a certificate holding part 56. A hardware characteristics information inspection part 62 extracts the hardware characteristics information incorporated in the certificate and detects whether it is coincident with the hardware characteristics information. An e-commerce part 64 performs commerce by using an inspected digital certificate.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－188873
（P2003－188873A）
(43)公開日　平成15年７月４日(2003.7.4)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/32		Ｇ０９Ｃ　1/00	６４０Ｅ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６４０	Ｈ０４Ｌ　9/00	６７５Ｂ	
			６７３Ｂ	

審査請求　未請求　請求項の数16　ＯＬ　（全 12 頁）

(21)出願番号　特願2001－380971(P2001－380971)

(22)出願日　平成13年12月14日(2001.12.14)

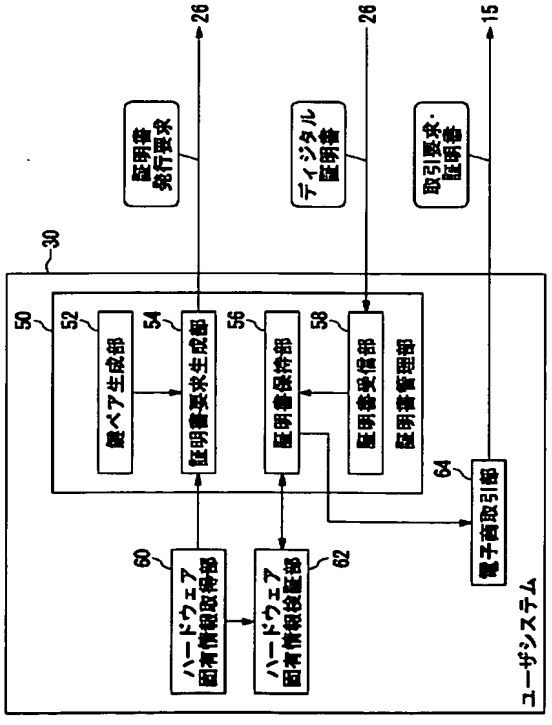
特許法第30条第１項適用申請有り　2001年10月31日～11月２日　社団法人情報処理学会　コンピュータセキュリティ研究会主催の「コンピュータセキュリティシンポジウム2001」において文書をもって発表

(71)出願人　593165487
学校法人金沢工業大学
石川県石川郡野々市町扇が丘７番１号
(72)発明者　服部　進実
石川県石川郡野々市町扇が丘７番１号　学校法人金沢工業大学内
(72)発明者　千石　靖
石川県石川郡野々市町扇が丘７番１号　学校法人金沢工業大学内
(74)代理人　100105924
弁理士　森下　賢樹

Ｆターム(参考)　5J104 AA07 KA02 KA05 KA10 MA01 PA10

(54)【発明の名称】　認証方法、およびその方法を利用可能な認証装置、ユーザシステムおよび認証システム

(57)【要約】
【課題】　電子商取引において、なりすましなどのユーザの不正行為を防止することは難しかった。
【解決手段】　ハードウェア固有情報取得部６０は、ユーザの利用するハードウェアに固有の識別情報を取得する。証明書要求生成部５４は、鍵ペア生成部５２により生成されたユーザの公開鍵と、当該ハードウェアの固有情報とをユーザ情報として認証装置２６に送信し、証明書受信部５８は認証装置２６からハードウェア固有情報が組み込まれたディジタル証明書を受信し、証明書保持部５６に保持する。ハードウェア固有情報検証部６２は、証明書に組み込まれたハードウェア固有情報を抽出し、当該ハードウェアの固有情報と一致するかどうか検証する。電子商取引部６４は、検証済みのディジタル証明書を用いて商取引を行う。



1

【特許請求の範囲】

【請求項１】　ユーザシステムからディジタル証明書の発行要求が出されたとき、そのユーザシステムで利用するハードウェアに固有の識別情報を組み込む形で当該証明書を生成し、そのユーザシステムへ発行することを特徴とする認証方法。

【請求項２】　前記ユーザシステムは、自己のハードウェアに固有の識別情報と照合して前記発行された証明書の正当性を検証した後、ネットワーク上の電子商取引の際にその証明書を利用することを特徴とする請求項１に記載の認証方法。

【請求項３】　ネットワーク上で前記ユーザシステムに所定のサービスを提供する組織が前記証明書の発行機関を兼ねることを特徴とする請求項１または２に記載の認証方法。

【請求項４】　前記ハードウェアに固有の前記識別情報を標準的なディジタル証明書の拡張領域に埋め込んで発行することを特徴とする請求項１から３のいずれかに記載の認証方法。

【請求項５】　前記ユーザシステムは、前記証明書の発行要求の際、自己のハードウェアに固有の識別情報を読み出し可能に設定することを特徴とする請求項１から４のいずれかに記載の認証方法。

【請求項６】　前記ユーザシステムは、前記証明書の発行要求に先立ち、ユーザに自己のハードウェアに固有の識別情報を読み出してよいかどうか問い合わせることを特徴とする請求項１から５のいずれかに記載の認証方法。

【請求項７】　ユーザシステムで利用するハードウェアに固有の識別情報を組み込む形でディジタル証明書を生成する証明書生成部と、
前記生成された証明書を前記ユーザシステムに発行する証明書発行部と、
前記証明書を保持する証明書データベースとを含むことを特徴とする認証装置。

【請求項８】　第３者から前記証明書の正当性を検証するための公開鍵を要求されたとき、前記証明書データベースから当該証明書の公開鍵を抽出して配布する公開鍵配布部をさらに含むことを特徴とする請求項７に記載の認証装置。

【請求項９】　ユーザが利用する自己のハードウェアに固有の識別情報を取得する取得部と、
前記自己のハードウェアに固有の識別情報を認証局に送信して、その識別情報を組み込んだディジタル証明書の発行を受け、その証明書を保持する証明書管理部と、
前記自己のハードウェアに固有の識別情報と照合して前記発行された証明書の正当性を検証する検証部とを含むことを特徴とするユーザシステム。

【請求項１０】　前記検証された証明書を利用して電子商取引を要求する取引部をさらに含むことを特徴とする

2

請求項９に記載のユーザシステム。

【請求項１１】　前記検証部により前記証明書の正当性が否定された場合、前記証明書を用いた電子商取引を禁止し、前記認証局にその旨を通知する警告部をさらに含むことを特徴とする請求項１０に記載のユーザシステム。

【請求項１２】　前記取得部は、前記自己のハードウェアに固有の識別情報の読み出し許可をユーザから得た上で、その識別情報を取得することを特徴とする請求項９から１１のいずれかに記載のユーザシステム。

【請求項１３】　ディジタル証明書を発行する認証装置と、前記証明書の発行を受けるユーザシステムとを含む認証システムであって、
前記認証装置は、
前記ユーザシステムで利用するハードウェアに固有の識別情報を受信し、その識別情報を組み込む形でディジタル証明書を生成する証明書生成部と、
前記生成された前記証明書を前記ユーザシステムに発行する証明書発行部と、
前記証明書を保持する証明書データベースとを含み、
前記ユーザシステムは、
ユーザが利用する自己のハードウェアに固有の識別情報を取得する取得部と、
前記自己のハードウェアに固有の識別情報を前記認証装置に送信して、その識別情報を組み込んだディジタル証明書の発行を受け、その証明書を保持する証明書管理部と、
前記自己のハードウェアに固有の識別情報と照合して前記証明書の正当性を検証する検証部とを含むことを特徴とする認証システム。

【請求項１４】　ユーザが利用する自己のハードウェアに固有の識別情報を取得するモジュールと、
前記自己のハードウェアに固有の識別情報を認証局に送信して、その識別情報を組み込んだディジタル証明書の発行を受け、その証明書を保持するモジュールと、
前記自己のハードウェアに固有の識別情報と照合して前記発行された証明書の正当性を検証するモジュールとを含むコンピュータ用のプログラム。

【請求項１５】　証明書発行の申請時に、ユーザシステムは自己が使用しているハードウェアの固有情報を含めた個人情報を認証局に送り、前記認証局は、その情報を付加した証明書を発行し、前記ユーザシステムは受け取ったディジタル証明書を使用して認証を行い、電子商取引を行うことを特徴とする認証システム。

【請求項１６】　前記ユーザシステム側でユーザの使用しているハードウェア情報と証明書に記録されているハードウェア情報を比較し、一致すれば、その証明書を前記電子商取引におけるサービス提供者側に送信し、前記サービス提供者側でその証明書の認証を行い、取引を開始することを特徴とする請求項１５に記載の認証システ

ム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明はユーザの不正行為を抑制する認証技術、とくにディジタル証明書を利用してユーザのなりすましなどの不正行為を抑制する認証方法およびその方法を利用可能な認証装置、ユーザシステムおよび認証システムに関する。

【０００２】

【従来の技術】近年、インターネット上での電子商取引が盛んに行われるようになってきている。その一つとしてオンラインショップを利用するオンラインショッピングがある。このオンラインショッピングはいわゆる「通信販売」であるが、インターネットを利用している人にとっては通信販売以上に簡単に商品を注文・購入できたり、サービスを受けたりすることができる有意義なものである。

【０００３】また電子署名を用いて各種公的手続きをネットワーク上で行うことも時代の趨勢であり、日本でも今年から電子署名法が施行され、電子政府構想が政策として掲げられている。近い将来、公的書類の申請や発行、税金等の手続きが電子的に行われるようになると期待されている。

【０００４】

【発明が解決しようとする課題】しかし、いくつかの問題点も抱えている。オンラインショッピングの問題には、電子商取引における不正行為が挙げられる。その不正行為には、オンラインショップ側の不正とユーザ側の不正がある。ショップ側の不正行為として、商品の未着、代金引換郵便の悪用などがある。またユーザ側の不正行為には、不当なＩＤ・パスワードの使用、クレジットカードの盗用などの「なりすまし」がある。

【０００５】不正に入手したユーザＩＤとパスワードを用いて海外からローミングサービスを利用したり、インターネットで利用したクレジットカード番号が盗用されるなどなりすましによる不正アクセス事件のニュースが数多く報告されている。そのような事件が多発する中で、オンラインショップ側の不正行為はショップを利用するユーザ側が注意することである程度防ぐことが出来るが、ユーザ側の不正行為を防ぐことは非常に困難であると考えられる。

【０００６】本発明はこうした状況に鑑みてなされたものであり、その目的は、ユーザの匿名性を残しつつ、ユーザを間接的に証明する情報を付加したディジタル証明書を利用して認証を行い、ユーザの不正行為を抑制する認証技術を提供することにある。

【０００７】

【課題を解決するための手段】本発明のある態様は認証方法に関する。この方法は、ユーザシステムからディジタル証明書の発行要求が出されたとき、そのユーザシステムで利用するハードウェアに固有の識別情報を組み込む形で当該証明書を生成し、そのユーザシステムへ発行する。

【０００８】前記ユーザシステムは、自己のハードウェアに固有の識別情報と照合して前記発行された証明書の正当性を検証した後、ネットワーク上の電子商取引の際にその証明書を利用してもよい。

【０００９】ネットワーク上で前記ユーザシステムに所定のサービスを提供する組織が前記証明書の発行機関を兼ねてもよい。この組織は、ユーザシステムにインターネットへの接続サービスを提供するインターネットサービスプロバイダであってもよい。またこの組織は専用線を引いている企業や団体であってもよい。このような組織はサービスをユーザに無償または有償で提供し、ユーザの個人情報を管理している。この証明書の発行機関は、前記ハードウェアに固有の前記識別情報を標準的なディジタル証明書の拡張領域に埋め込んで発行してもよい。ハードウェアに固有の識別情報は、ユーザシステムと証明書の発行機関との間で一意性が保証されるものであってもよい。

【００１０】前記ユーザシステムは、前記証明書の発行要求の際、自己のハードウェアに固有の識別情報を読み出し可能に設定してもよい。前記ユーザシステムは、前記証明書の発行要求に先立ち、ユーザに自己のハードウェアに固有の識別情報を読み出してよいかどうか問い合わせてもよく、ユーザが読み出しを許可した場合に、識別情報の読み出しが可能になるように設定を行ってもよい。

【００１１】本発明の別の態様は認証装置に関する。この装置は、ユーザシステムで利用するハードウェアに固有の識別情報を組み込む形でディジタル証明書を生成する証明書生成部と、前記生成された証明書を前記ユーザシステムに発行する証明書発行部と、前記証明書を保持する証明書データベースとを含む。第３者から前記証明書の正当性を検証するための公開鍵を要求されたとき、前記証明書データベースから当該証明書の公開鍵を抽出して配布する公開鍵配布部をさらに含んでもよい。

【００１２】本発明のさらに別の態様はユーザシステムに関する。このユーザシステムは、ユーザが利用する自己のハードウェアに固有の識別情報を取得する取得部と、前記自己のハードウェアに固有の識別情報を認証局に送信して、その識別情報を組み込んだディジタル証明書の発行を受け、その証明書を保持する証明書管理部と、前記自己のハードウェアに固有の識別情報と照合して前記発行された証明書の正当性を検証する検証部とを含む。

【００１３】前記検証された証明書を利用して電子商取引を要求する取引部をさらに含んでもよい。前記検証部により前記証明書の正当性が否定された場合、前記証明書を用いた電子商取引を禁止し、前記認証局にその旨を

通知する警告部をさらに含んでもよい。

【００１４】前記取得部は、前記自己のハードウェアに固有の識別情報の読み出し許可をユーザから得た上で、その識別情報を取得してもよい。

【００１５】本発明のさらに別の態様は認証システムに関する。この認証システムは、前述の認証装置とユーザシステムとを含む。

【００１６】本発明のさらに別の態様はコンピュータ用のプログラムに関する。このプログラムは、ユーザが利用する自己のハードウェアに固有の識別情報を取得するモジュールと、前記自己のハードウェアに固有の識別情報を認証局に送信して、その識別情報を組み込んだディジタル証明書の発行を受け、その証明書を保持するモジュールと、前記自己のハードウェアに固有の識別情報と照合して前記発行された証明書の正当性を検証するモジュールとを含む。

【００１７】本発明のさらに別の態様も認証システムに関する。証明書発行の申請時に、ユーザシステムは自己が使用しているハードウェアの固有情報を含めた個人情報を認証局に送り、前記認証局は、その情報を付加した証明書を発行し、前記ユーザシステムは受け取ったディジタル証明書を使用して認証を行い、電子商取引を行う。前記ユーザシステム側でユーザの使用しているハードウェア情報と証明書に記録されているハードウェア情報を比較し、一致すれば、その証明書を前記電子商取引におけるサービス提供者側に送信し、前記サービス提供者側でその証明書の認証を行い、取引を開始してもよい。

【００１８】なお、以上の構成要素の任意の組合せ、本発明の表現を方法、装置、サーバ、システム、コンピュータプログラム、記録媒体などの間で変換したものもまた、本発明の態様として有効である。

【００１９】

【発明の実施の形態】本発明の目的は、電子商取引において、ユーザ側の不正行為である「なりすまし」を事前に防ぐことである。このなりすましは、インターネット上での高い匿名性という性質を悪用した行為であるが、実施の形態ではユーザの匿名性は残しつつユーザの不正行為を抑制する方法を提案する。

【００２０】現在、Ｗｅｂでは幾つかの認証システムが利用されている。主なものにインターネットを通じて安全にクレジットカード決済を行うためのＳＥＴ（Secure Electronic Transactions）や米国マサチューセッツ工科大学でのＡｔｈｅｎａプロジェクトの一部として設計された認証システムであるＫｅｒｂｅｒｏｓなどがある。

【００２１】これらの認証システムは通信中のデータの安全を確保するためのシステムであり、ユーザ自身が不正なユーザアカウントやパスワードを使用していることを検出するのは困難であり、また不正行為を検出した場合でもそのユーザを突き止めることは困難である。

【００２２】不正行為を抑制するためにはユーザの個人情報を公開すればいいが、ある程度個人の匿名性を残すために、直接的にはユーザを知ることができないが間接的にはユーザを知ることのできる情報を公開することとする。公開する情報は第三者によって改竄されたり、盗用されないようにディジタル証明書を使用する。そのユーザを間接的に知ることができる情報をディジタル証明書に付加して利用し、ユーザの認証を行うことによりユーザの不正行為を抑制させる。つまり、善良なサービス提供者である店舗を保護しながら、ユーザが安全な電子商取引を行うためのＷｅｂ認証システムを提案する。

【００２３】実施の形態に係る認証システムを説明する前に、既存の認証システムを説明する。認証システムは多くの種類が存在しているが、それらのシステムで用いられている既存の認証方法は次のように分類できる。

【００２４】（１）変形パスワード

パスワードを一方向性関数を通して処理し、ホストが記憶していたパスワードに同じ関数を適用し、２つを比較することにより認証を行う。通信中の盗聴を防ぐ。

【００２５】（２）チャレンジ応答

ホストがユーザにチャレンジと呼ぶランダム値を送り、その値を一方向性関数で計算し、返答とともに戻す。暗号化されたパスワードをそのまま用いる再生攻撃に対抗する。

【００２６】（３）タイムスタンプ

認証要求時に現在の日時を用いる。すべてのシステムが安全で同期がとれている時計を持っている必要がある。

【００２７】（４）ワンタイムパスワード

変形パスワードの一種で、パスワードに一方向性関数を用いて一度しか使えないパスワードを生成する。盗聴と再生攻撃の両方に対抗する。

【００２８】（５）ゼロ知識法

会話型証明システムに基づく暗号技術のひとつである。

【００２９】（６）ディジタル署名またはディジタル証明書

認証プロトコルの基本である。データの一部をユーザの私有鍵を用いて署名し、私有鍵の持ち主であることを証明する。

【００３０】また、主な認証システムとして、ＳＥＴとＫｅｒｂｅｒｏｓが挙げられる。ＳＥＴは、インターネットを通じて安全にクレジットカード決済を行うための技術仕様である。大手クレジットカード会社のほか、コンピュータ関連企業が協同で規格を策定している。ＳＥＴの使用目的は、クレジットカード番号がショップに知られないようにすることである。

【００３１】ユーザがＳＥＴを利用するには、専用ソフトウェアをダウンロードしなければならず、そのソフトウェアをユーザが入手するにはＷｅｂ上でのＳＥＴ利用申請が必要で、その申請にはインターネット上で情報を

暗号化して送受信するプロトコルであるＳＳＬ（Secure Socket Layer）が利用されている。また、専用ソフトウェアさえ使用していれば正規のユーザとみなされる。

【００３２】したがってＳＥＴには、（１）専用のソフトウェアを使用する必要がある、（２）正規ユーザ認証が申請時すなわち専用ソフトダウンロード時の一回だけである、（３）汎用性があまりないなどの問題があり、「なりすまし」の対策が不十分であると考えられる。

【００３３】Ｋｅｒｂｅｒｏｓとは、マサチューセッツ工科大学のＡｔｈｅｎａプロジェクトで開発されたネットワーク上での利用を前提としたユーザ認証方式のことである。Ｋｅｒｂｅｒｏｓ認証では、認証サーバ（ＡＳ：Authentication Server）と鍵配布サーバ(ＴＧＳ：Ticket Granting Server)の２つのサーバによって認証が行なわれ、通信の秘匿やユーザ認証などをすべて共通鍵暗号で実現しているのが特徴である。

【００３４】ＳＥＴやＫｅｒｂｅｒｏｓは通信中にID・パスワードや秘密情報が傍受されることを防いでいるが、秘密情報が盗まれてしまえば機能しなくなる。だが、次に述べる実施形態の認証システムでは、ユーザの使用しているハードウェアに関する情報を基に認証を行うため、ハードウェア自身が盗まれない限り、安全に認証を行える。情報が盗まれた時よりも、物自体が盗まれた時の方が発見が早いので、本実施形態の認証システムでは不正行為による被害を最小限に止めることが出来る。

【００３５】本認証システムは、ディジタル証明書を利用したＷｅｂ認証システムである。ディジタル証明書にユーザを間接的に知ることの出来る情報を新たに付加することにより、認証を強化する。ユーザを間接的に知る情報として、ユーザが使用しているハードウェアの固有な情報を利用することとする。そのハードウェア固有情報を証明書に付加して、接続時に証明書による認証を行う。

【００３６】本認証システムで使用するディジタル証明書は、Ｘ．５０９バージョン３証明書に準拠している。

【００３７】標準公開鍵証明書の形式であるＸ．５０９証明書形式は、次のようなものである。

（１）ＩＳＯ（国際標準化機構）、ＩＥＣ（国際電気標準会議）、ＩＴＵ（国際電気通信連合）が定めた標準公開鍵証明書形式である。

（２）１９８８年にバージョン１が開発され、現在はバージョン３が使用されている。

（３）バージョン３において拡張領域が追加されている。

（４）他の機能として証明書の有効期限等を設定することができ、扱いやすいディジタル証明書である。

【００３８】また、Ｘ．５０９証明書の構造は次のようになっている。なお以下においてＸ．５００とは、データ通信網、特にメッセージ通信網におけるディレクトリ機能を標準化することを目指してＩＴＵ－Ｔが１９８８年に勧告したものであり、Ｘ．５０９証明書では、認証局や証明書の保持者などのエンティティの名前として、このＸ．５００標準を用いてインターネット全体での一意性を保つ。

【００３９】１．証明書バージョン
Ｘ．５０９による証明書のバージョン番号
２．証明書シリアル番号
認証局より任意に割り当てられた番号
３．アルゴリズム識別子
証明書発行者の署名用のディジタル署名アルゴリズムの識別子
４．認証局のＸ．５００名前
発行者である認証局のＸ．５００名前
５．有効期限
証明書の開始および終了日時
６．主体者のＸ．５００名前
証明される公開鍵と相関する私有鍵の保有者のＸ．５００名前
７．主体者の公開鍵情報
主体者すなわち証明書使用者の公開鍵値とそれに使われているＲＳＡ、楕円暗号等のアルゴリズムの識別子
８．認証局の識別子
証明書を発行する認証局の名前があいまいにならないようにするために用いるオプションビット列
９．主体者の識別子
主体者の名前があいまいにならないように用いるオプションビット列
１０．拡張
拡張領域
１１．認証局のディジタル署名
ハッシュアルゴリズムを用いて証明書のダイジェストすなわち指紋に相当するデータをとり、そのダイジェストを認証局の秘密鍵によって暗号化したもの。

【００４０】図１は、Ｘ．５０９証明書に含まれるこれらのデータの構造を説明する図である。本認証システムは、Ｘ．５０９証明書の拡張領域にハードウェア固有情報を付加した独自の証明書による認証を行う。

【００４１】本認証システムにおいて、ディジタル証明書に付加するハードウェア情報は以下のものを利用する。

（１）ＰＳＮ（Processor Serial Number）

（２）ＭＡＣアドレス（Media Access Control Address）、ＩＰアドレス（Internet Protocol Address）

【００４２】ＭＡＣアドレスやＩＰアドレスの情報は不正に書き換えられる恐れがあるため、書き換え不可能で固有のハードウェア情報であるＰＳＮを利用することが重要である。

【００４３】ＰＳＮはＩｎｔｅｌ社がペンティアム３（登録商標）以降のマイクロプロセッサに搭載したプロ

セッサ固有の識別番号である。すべてのチップに違う番号が割り当てられ、コンピュータの識別に使われる。

【００４４】このＰＳＮを表示及び使用するには、インテルプロセッサシリアルナンバーコントロールユーティリティ（Intel Processor Serial Number Control Utility）を使用する。ＢＩＯＳの設定で無効になっていれば、マザーボードの「Processor Number Feature」を「Enabled」にしておかなければ、警告のダイアログが表示され「無効」のままである。

【００４５】図２のように、プロセッサシリアルナンバーコントロールユーティリティを起動すると、ＢＩＯＳの設定が有効になっていれば、９６ビットのプロセッサシリアルナンバーが表示される。

【００４６】ＭＡＣアドレスとは、各Ｅｔｈｅｒｎｅｔ（登録商標）カードに固有のＩＤ番号である。全世界のＥｔｈｅｒｎｅｔカードには１枚１枚固有の番号が割り当てられており、これを元にカード間のデータの送受信が行われる。

【００４７】ＩＰアドレスは、インターネットやイントラネットなどのＩＰネットワークに接続されたコンピュータ１台１台に割り振られた識別番号である。

【００４８】本認証システムはＷｅｂ上での電子商取引で使用することにより、電子商取引での不正行為の一つである「なりすまし」の抑制を目的としている。なりすまし等の不正行為を抑制させるために、ディジタル証明書にユーザを間接的に知ることの出来るハードウェア固有情報を付加させている。しかし、これだけでは不正行為を抑止することは困難であり、ハードウェア固有情報を付加したディジタル証明書を使用した認証システムを効果的に運用・利用する必要がある。

【００４９】ユーザの不正行為を抑制させるために認証システムを効果的に運用するには、ＩＳＰ（Internet Services Provider）や専用線を引いている各種団体を認証局（ＣＡ：Certificate Authority）として利用する方法が考えられる。ほとんどのユーザは各自のコンピュータをインターネットに接続するためにＩＳＰや専用線を引いている各種団体を利用しているため、ＩＳＰや専用線を引いている各種団体をＣＡとして証明書の発行・管理を行う。

【００５０】ＩＳＰや各種団体等がＣＡとなることで、証明書を持っているユーザの身元を管理することが容易である。また、ＣＡ機関を新たに設ける必要がないため、コストや普及の面でもメリットがある。

【００５１】また、ＩＳＰや各種団体等に不正防止の責任義務を持たせることで、ユーザの不正行為をさらに抑制することが出来ると考えられる。

【００５２】本認証システムは、主にＷｅｂ上の電子商取引での利用を目的としている。つまり、Ｗｅｂ上のオンラインショッピングで、ユーザが不正行為を行わないようにするための認証システムである。

【００５３】図３は、ディジタル証明書の申請と発行の手順を説明する図である。まず、ユーザはユーザ自身が所属しているＩＳＰ等に証明書発行の申請をする。その申請時に、ユーザは自身が使用しているコンピュータのＭＡＣアドレス、ＰＳＮを含めた個人情報をＣＡであるＩＳＰに送る。ＣＡは、その情報を基に証明書を発行する。そして、ユーザは受け取ったディジタル証明書を使用して認証を行い、電子商取引を行う。

【００５４】図４は、認証システムにおける商取引の手順を説明する図である。サービスを提供する側であるオンラインショッピング店舗等は、利用者が接続して送信してくるディジタル証明書を基に利用者の認証を行い、取引を行う。

【００５５】ＣＡより発行されたディジタル証明書は、ユーザ側のコンピュータ内で保存管理される。例え不正をしようとしても、ディジタル証明書は改竄されたり不正生成されることはない。

【００５６】図５は、証明書の管理と認証の手順を説明する図である。ユーザがオンラインショッピングなどを利用する時、まずユーザ側でユーザの使用しているハードウェア情報と証明書に記録されているハードウェア情報を比較する。一致すれば、その証明書をサービス提供者側に送信する。受け取った提供者側でその証明書の認証を行い、取引を開始する。

【００５７】これらの動作は、ユーザ、サービス提供者共に本認証システムの専用ソフトウェアで行う事とする。この専用ソフトウェアはＣＡによって完全性を認証する。

【００５８】本認証システムの仕様をまとめると以下の通りである。

（１）ディジタル証明書を利用した認証システム。

（２）ディジタル証明書形式はＩＳＯ／ＩＥＣ／ＩＴＵが定めたＸ．５０９標準バージョン３を使用。

（３）ディジタル証明書の拡張としてコンピュータ固有の情報を付加させる。

（４）固有の情報としてＰＳＮ、ＭＡＣアドレス、ＩＰアドレスを使用する。

（５）プラットフォームはパーソナルコンピュータの標準的なＯＳである。

（６）ソフトウェアは標準的なＣ＋＋言語の開発環境で開発される。

（７）ＩＳＰや専用線を引いている各種団体をＣＡとすることで、不正行為抑制を強化。

【００５９】図６は、実施の形態に係る認証システムの構成図である。オンラインショッピングサイト１０は、オンラインにより商品の販売を行うサイトであり、Ｗｅｂサーバ１２、データベースサーバ１４、およびショップシステム１５を含む。ユーザはＷｅｂサーバ１２にアクセスして商品の閲覧、購入の申し込みができる。データベースサーバ１４はＷｅｂサーバ１２と連携して商品

の購入履歴の管理やユーザの個人情報の管理などを行う。ショップシステム１５は、証明書を利用したユーザ認証を行う専用ソフトウェアである。このショップシステム１５は、Ｗｅｂサーバ１２またはデータベースサーバ１４の機能の一部として設けられてもよい。なおオンラインショッピングサイト１０にはファイアウオールなどの機能が当然に含まれるが、ここでは図示しない。

【００６０】インターネットサービスプロバイダ１８は、ユーザ端末２８にインターネット１６へのアクセス環境を提供するものであり、メールサーバ２０、ＤＮＳサーバ２２、プロキシサーバ２４、および認証装置２６を含む。ユーザ端末２８は図示しないアクセスポイントにダイアルアップなどで接続し、インターネットサービスプロバイダ１８が提供する電子メール、インターネットアクセスなどのサービスを利用する。またユーザ端末２８に搭載された専用ソフトウェアであるユーザシステム３０は、インターネットサービスプロバイダ１８内の認証装置２６と通信して証明書の発行を受ける。このようにインターネットサービスプロバイダ１８はユーザ端末２８を認証する認証局としての機能を兼ね備える。

【００６１】図７は、認証装置２６の構成図である。この構成は、ハードウェア的には、任意のコンピュータのＣＰＵ、メモリ、その他のＬＳＩで実現でき、ソフトウェア的にはメモリにロードされた認証機能のあるプログラムなどによって実現されるが、ここではそれらの連携によって実現される機能ブロックを描いている。したがって、これらの機能ブロックがハードウェアのみ、ソフトウェアのみ、またはそれらの組合せによっていろいろな形で実現できることは、当業者には理解されるところである。

【００６２】証明書生成部３２は、ユーザシステム３０から証明書発行要求を受け取り、ディジタル証明書を生成する。ユーザシステム３０から受け取る証明書発行要求には、ユーザの利用するハードウェアすなわちユーザ端末２８に固有の識別情報が含まれる。

【００６３】証明書生成部３２は、鍵生成部３４、ダイジェスト生成部３６、およびディジタル署名部３８を含む。ダイジェスト生成部３６は証明書データをハッシュ関数に通してダイジェストを取得する。証明書データは、証明者情報、認証局情報、ユーザ情報、および拡張情報を含む。証明者情報は、図１で説明した（１）証明書バージョン、（２）証明書シリアル番号、（３）アルゴリズム識別子、および（５）有効期限のデータであり、認証局情報は、（４）認証局のＸ．５００名前および（８）認証局の識別子のデータである。ユーザ情報は、（６）主体者のＸ．５００名前、（７）主体者の公開鍵情報、および（９）主体者の識別子のデータである。また拡張情報は、（１０）拡張領域のデータである。また拡張情報にはユーザシステム３０から受け取ったハードウェア固有情報が含まれる。したがって、証明書データにはユーザが利用しているハードウェアの固有情報が組み込まれている。

【００６４】ディジタル署名部３８は、鍵生成部３４が生成した当該認証局の秘密鍵を用いて、ダイジェスト生成部３６により生成されたダイジェストを暗号化してディジタル署名を生成し、その署名データを図１のように証明書データに追加する。なお鍵生成部３４が生成した当該認証局の公開鍵と秘密鍵のペアは証明書データベース４２に保持される。証明書発行部４０は、このようにして生成されたディジタル証明書を証明書データベース４２に保持するとともに、ユーザシステム３０へ発行する。

【００６５】公開鍵配布部４４は、ショップシステム１５から当該認証局の公開鍵の要求を受けつけ、証明書データベース４２から当該認証局の公開鍵を取得してショップシステム１５へ送信する。

【００６６】図８は、ユーザシステム３０の構成図である。この構成図は、ソフトウェアとハードウェアの連携によって実現される機能ブロックを描いたものであり、これらの機能ブロックは、ユーザ端末２８にインストールされるアプリケーションプログラムとして実現されてもよく、少なくとも一部がオペレーションシステムやファームウェアの機能を用いて実現されたり、ハードウェアを用いて実現されてもよい。

【００６７】証明書管理部５０は、認証装置２６へ証明書発行要求を送信し、認証装置２６からディジタル証明書を受信して管理する。証明書管理部５０は、鍵ペア生成部５２、証明書要求生成部５４、証明書保持部５６、および証明書受信部５８を含む。鍵ペア生成部５２は、ユーザ固有の公開鍵と秘密鍵のペアを生成する。生成された鍵は図示しない記憶部に保持される。ハードウェア固有情報取得部６０は、当該ユーザシステム３０がインストールされたハードウェアすなわちユーザ端末２８に固有の識別情報を取得する。このハードウェア固有の識別情報の一例は、前述のＰＳＮであり、ＭＡＣアドレス、ＩＰアドレスなどで代用したり、組合せてもよい。

【００６８】証明書要求生成部５４は、鍵ペア生成部５２により生成された公開鍵と、ハードウェア固有情報取得部６０により取得されたハードウェア固有情報とをユーザ情報として用いた証明書発行要求を生成し、認証装置２６にその要求を送信する。

【００６９】証明書受信部５８は認証装置２６が発行したディジタル証明書を受信し、証明書保持部５６がそのディジタル証明書を保持する。ハードウェア固有情報検証部６２は、証明書保持部５６に保持されたディジタル証明書に組み込まれたハードウェア固有情報を抽出し、ハードウェア固有情報取得部６０により取得された自己のハードウェア固有情報と比較し、両者が一致するかどうかを検証する。電子商取引部６４は、ショップシステム１５との間で電子商取引を開始する際、証明書保持部

５６に保持された検証済みのディジタル証明書をショップシステム１５に送信する。ショップシステム１５は後述のようにユーザシステム３０から送信されたディジタル証明書を検証して、電子商取引部６４に取引の開始確認を返信する。これを受けて電子商取引部６４はショップシステム１５との間で商取引を行う。

【００７０】ハードウェア固有情報検証部６２による検証の結果、ディジタル証明書に含まれるハードウェア固有情報と当該ユーザ端末２８のハードウェア固有情報とが一致しなかった場合、ハードウェア固有情報検証部６２はそのディジタル証明書が不正に入手されたものと判断して無効化し、電子商取引部６４による商取引に使用されないように制限する。またそのような場合、認証局に不正があることを通知する警告部がさらに設けられてもよい。

【００７１】図９は、ショップシステム１５の構成図である。電子商取引部７０は、ユーザシステム３０からディジタル証明書とともに取引要求を受け取る。ＣＡ公開鍵管理部７４は、ディジタル証明書を発行した認証装置２６に対してＣＡ固有の公開鍵を要求し、認証装置２６からそのＣＡ公開鍵を受け取る。証明書検証部７２は、ＣＡ公開鍵を用いて、電子商取引部７０が受信したディジタル証明書を復号し、証明書の正当性を検証する。証明書が検証されると、電子商取引部７０はユーザシステム３０へ取引開始確認を送信する。これ以降、電子商取引部７０はユーザシステム３０との間で商取引を行う。証明書の正当性が確認されなかった場合は、ユーザシステム３０の取引要求を拒否する。

【００７２】図１０～図１３を参照して、実施の形態に係る認証システムによる認証手順を説明する。図１０は、認証装置２６におけるディジタル証明書の生成と発行の手順を示すフローチャートである。証明書生成部３２はユーザから証明書発行要求を受信する（Ｓ１０）。この発行要求にはユーザが利用しているハードウェアに固有の識別情報が含まれている。ダイジェスト生成部３６は、このハードウェア固有情報を含むディジタル証明書のデータをハッシュ関数に通してダイジェストを生成する（Ｓ１２）。ダイジェストはディジタル証明書の「指紋」に相当する。ディジタル署名部３８は当該認証局の秘密鍵を用いてこのダイジェストを暗号化して署名データを作成し、ディジタル証明書に付加する（Ｓ１４）。証明書発行部４０はこうして得られたディジタル証明書を発行する（Ｓ１６）。

【００７３】図１１は、ユーザシステム３０における証明書発行要求の手順を示すフローチャートである。鍵ペア生成部５２はユーザ固有の公開鍵と秘密鍵のペアを生成する（Ｓ２０）。ハードウェア固有情報取得部６０はハードウェア固有情報を読み出してもよいかどうかユーザに問い合わせる（Ｓ２２）。ユーザが読み出しを許可した場合（Ｓ２２のＹ）、ハードウェア固有情報取得部６０はハードウェア固有情報を取得する（Ｓ２４）。証明書要求生成部５４は取得したハードウェア固有情報とユーザの公開鍵データをユーザ情報として含むディジタル証明書の発行要求を認証装置２６に送信する（Ｓ２６）。ステップＳ２２でユーザが読み出しを許可しない場合（Ｓ２２のＮ）、ハードウェア固有情報の読み出しおよび証明書の発行要求をすることなく、終了する。

【００７４】なお、鍵の生成（Ｓ２０）は証明書の発行要求のたびに行う必要はなく、一度生成した鍵を何度も用いてよい。またハードウェア固有情報の読み出しの問い合わせ（Ｓ２２）についても、ユーザが一度読み出しを許可すると、再度の問い合わせをしないようにしてもよい。またハードウェア固有情報の読み出しができないようにロックをかけ、ユーザが読み出しの許可を与えた場合にそのロックを解除して自由に読み出し可能にするロック制御部をさらに設けてもよい。

【００７５】図１２は、ユーザシステム３０におけるハードウェア固有情報の検証手順を示すフローチャートである。認証装置２６からディジタル証明書が受信されると、ＣＡの公開鍵を用いてその証明書の正当性が検証される（Ｓ３０）。ハードウェア固有情報検証部６２は証明書からハードウェア固有情報を抽出する（Ｓ３２）。ハードウェア固有情報取得部６０は当該ユーザシステム３０が利用するハードウェアから自己のハードウェア固有情報を取得する（Ｓ３４）。ハードウェア固有情報検証部６２は、証明書から抽出されたハードウェア固有情報と自己のハードウェア固有情報とを比較し、一致するかどうかを調べる（Ｓ３６）。一致する場合（Ｓ３６のＹ）、電子商取引部６４は商取引の要求の際、そのディジタル証明書をショップシステム１５に送信し（Ｓ３８）、一致しない場合（Ｓ３６のＮ）、ディジタル証明書の送信を行わない。一致しない場合、そのディジタル証明書は不正に入手されたものである可能性があるため、その証明書を発行したＣＡである認証装置２６に不正があることを警告するステップをさらに含んでもよい。

【００７６】図１３は、ショップシステム１５におけるディジタル証明書の検証手順を示すフローチャートである。電子商取引部７０はユーザシステム３０から取引要求とともにユーザの証明書を受信する（Ｓ４０）。ＣＡ公開鍵管理部７４は受信した証明書の完全性を検証するために、証明書を発行したＣＡである認証装置２６へ公開鍵を要求する（Ｓ４２）。証明書検証部７２はＣＡ公開鍵により証明書のディジタル署名を復号し、署名を検証する（Ｓ４２）。ＣＡの署名の正当性が検証された場合（Ｓ４２のＹ）、電子商取引部７０はユーザシステム３０に取引開始確認を送信し、ユーザシステム３０との取引を実行し（Ｓ４４）、ＣＡの署名の正当性が否定された場合（Ｓ４２のＮ）、ユーザシステム３０との取引を拒否する（Ｓ４６）。

15

【００７７】ユーザシステム３０とショップシステム１５は、ユーザとオンラインショップとの間の電子商取引をディジタル証明書を用いて安全に行うための専用ソフトウェアとして実現することができる。この場合、とくにユーザ端末２８側にインストールされるユーザシステム３０のプログラムは、ハードウェア固有情報の検証ルーチンが不正に改変されないようにプログラムコードの難読化などの改変防止対策が取られる。

【００７８】以上述べたように、本認証システムは、ユーザが使用しているハードウェア情報を付加したディジタル証明書を使用して認証を行うシステムである。主に電子商取引での利用を目的としている。なぜなら、セキュリティに関心がないユーザがコンピュータを使ってインターネットに接続してオンラインショッピングを楽しんでおり、ユーザ自身が扱うＩＤ・パスワードが簡単に漏れてしまうことが多く、不正行為も容易に出来てしまうからである。それを抑制するためにコンピュータ側で認証情報を管理する必要がある。ＩＤ・パスワードだけの認証情報では不正行為を抑止することは困難であるため、不変なユーザ情報としてＰＳＮ、ＭＡＣアドレス等のハードウェア固有情報を用いた。本認証システムを利用することで、サービスを提供する側もユーザ自身もより安全で容易に電子商取引を行うことができる。

【００７９】また本認証システムは、標準的なＯＳの上にアプリケーションレベルで開発できるため、実装に手間がかからず、またＩＣカードによる認証や指紋認証とは違い、認証のための特別なハードウェアを必要としない。また本認証システムではユーザが使用するハードウェアが盗まれない限り、「なりすまし」ができない。ユーザは認証データを盗まれて気がつかないが、自分の使っているハードウェアの盗難は早期に発見できるため、不正利用に対して直ちに対処できる。

【００８０】また本認証システムでは、ユーザの個人情報を管理してユーザにネットワークサービスを提供するＩＳＰなどの組織が認証局は兼ねるため、ユーザの属する組織ごとに分散された認証局を比較的簡単な構成で立ち上げることができる。

【００８１】以上、本発明を実施の形態をもとに説明した。実施の形態は例示であり、それらの各構成要素や各処理プロセスの組合せにいろいろな変形例が可能なこと、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。以下そのような変形例を説明する。

【００８２】本認証システムはＰＣベースのシステムに限られない。ＰＣの普及率は飽和状態にあり、その代わり携帯端末の普及が目覚しい。本システムはＰＤＡ（Personal Digital Assistance）と総称される携帯端末機や、携帯電話に応用することができる。最近、一部の携帯電話でＪａｖａ（登録商標）アプリケーションが動作するようになってきており、今後全ての携帯電話の標準的な機能となると思われる。また、各携帯電話は必ず固有ＩＤを持っており、この固有情報とＪａｖａ技術を利用することにより、ディジタル証明書を利用した認証システムを構築することができる。

16

【００８３】また上記では一般的な例としてＷｅｂ上での電子商取引においてディジタル証明書を利用する場合を説明したが、もちろんＷｅｂに限定する趣旨ではない。またディジタル証明書は電子商取引に限らず、公的書類の申請や発行、税金等の手続きなど商取引以外の場面でも利用される。そのような場合においても本発明の認証システムを適用することにより、なりすましなどの不正行為を防止することができる。

【００８４】また本認証システムはユーザの属する組織単位で分散した認証局を用いるため、ユーザ全体を統一して管理する必要はなく、認証局ごとに異なる認証方式を採用することもできる。また組織単位でユーザを認証可能であればよいので、組織内でユーザをユニークに識別できる固有の識別情報をディジタル証明書に用いることで十分である。したがってＰＳＮのように完全にユニークな識別情報を使わなくても、ＭＡＣアドレスやハードウェアのシリアルナンバー、ハードウェアのコンフィグレーションなど、他の識別情報を組合せたり、それらの識別情報の一部を用いることで対処することも可能である。また識別情報として、ＢＩＯＳのバージョンやＲＯＭに書き込まれた製品のロットナンバーなどを用いてもよい。

【００８５】

【発明の効果】本発明によれば、ユーザ認証における不正行為を防止することができる。

【図面の簡単な説明】

【図１】　実施の形態に係るディジタル証明書のデータの構造を説明する図である。

【図２】　プロセッサシリアルナンバーの表示画面を説明する図である。

【図３】　実施の形態に係るディジタル証明書の申請と発行の手順を説明する図である。

【図４】　実施の形態に係る認証システムにおける商取引の手順を説明する図である。

【図５】　実施の形態に係る証明書の管理と認証の手順を説明する図である。

【図６】　実施の形態に係る認証システムの構成図である。

【図７】　図６の認証装置の構成図である。

【図８】　図６のユーザシステムの構成図である。

【図９】　図６のショップシステムの構成図である。

【図１０】　認証装置におけるディジタル証明書の生成と発行の手順を示すフローチャートである。

【図１１】　ユーザシステムにおける証明書発行要求の手順を示すフローチャートである。

【図１２】　ユーザシステムにおけるハードウェア固有

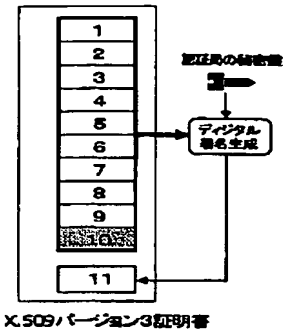
情報の検証手順を示すフローチャートである。

【図１３】 ショップシステムにおけるディジタル証明書の検証手順を示すフローチャートである。

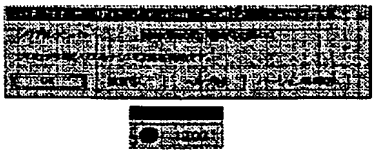
【符号の説明】

１０ オンラインショッピングサイト、 １２ Ｗｅｂサーバ、 １４ データベースサーバ、 １５ ショップシステム、 １６ インターネット、 １８インターネットサービスプロバイダ、 ２６ 認証装置、 ２８ ユーザ端末、 ３０ ユーザシステム、 ３２ 証明書生成部、 ３４ 鍵生成部、 ３６ダイジェスト生成部、 ３８ ディジタル署名部、 ４０ 証明書発行部、４２ 証明書データベース、 ４４ 公開鍵配布部、 ５０ 証明書管理部、５２ 鍵ペア生成部、 ５４ 証明書要求生成部、 ５６ 証明書保持部、 ５８ 証明書受信部、 ６０ ハードウェア固有情報取得部、 ６２ ハードウェア固有情報検証部、 ６４ 電子商取引部、 ７０ 電子商取引部、 ７２ 証明書検証部、 ７４ ＣＡ公開鍵管理部。

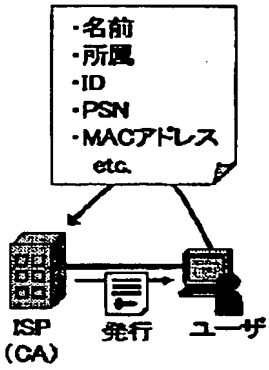
【図１】



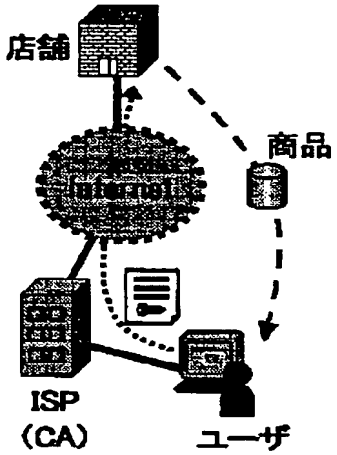
【図２】



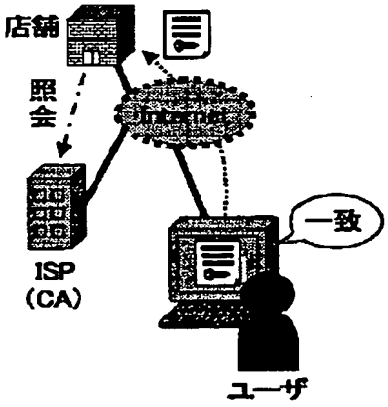
【図３】



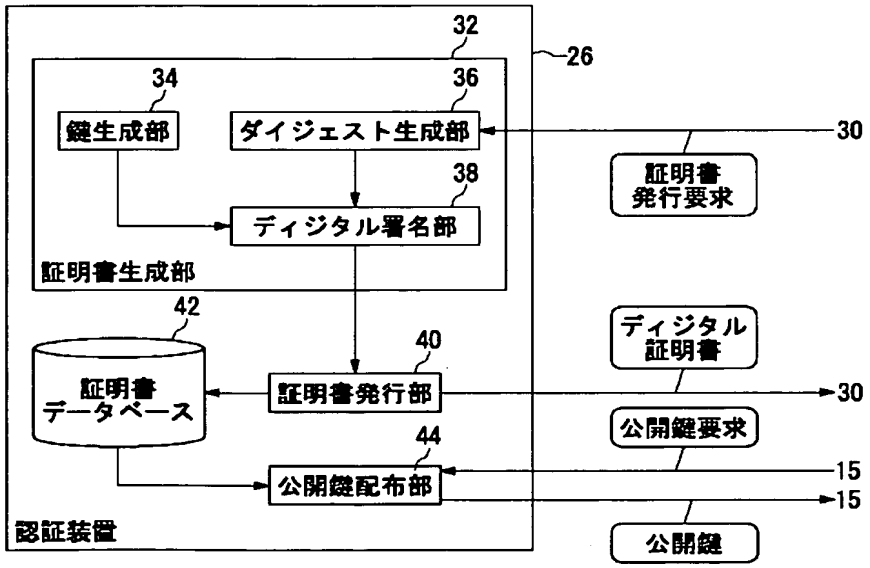
【図４】



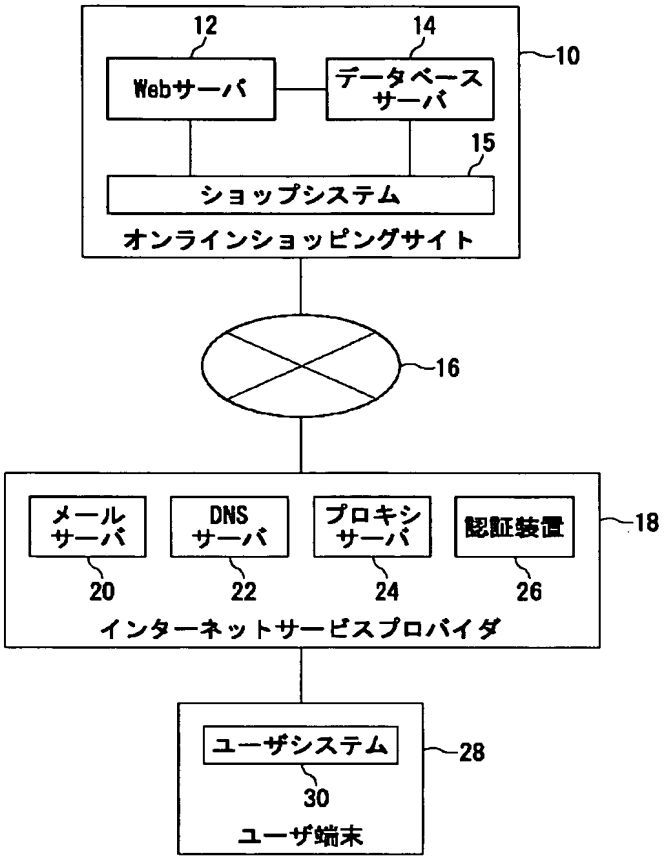
【図５】



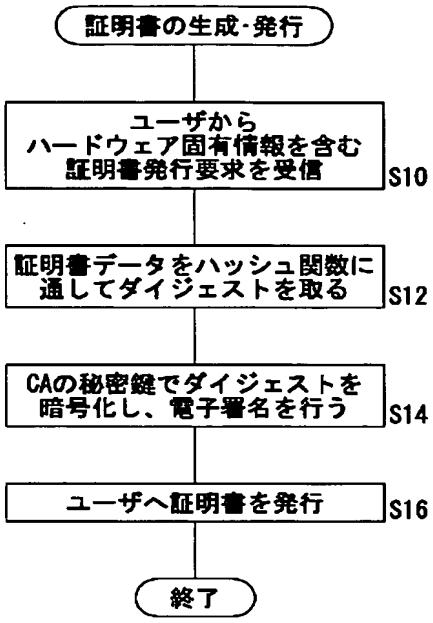
【図７】



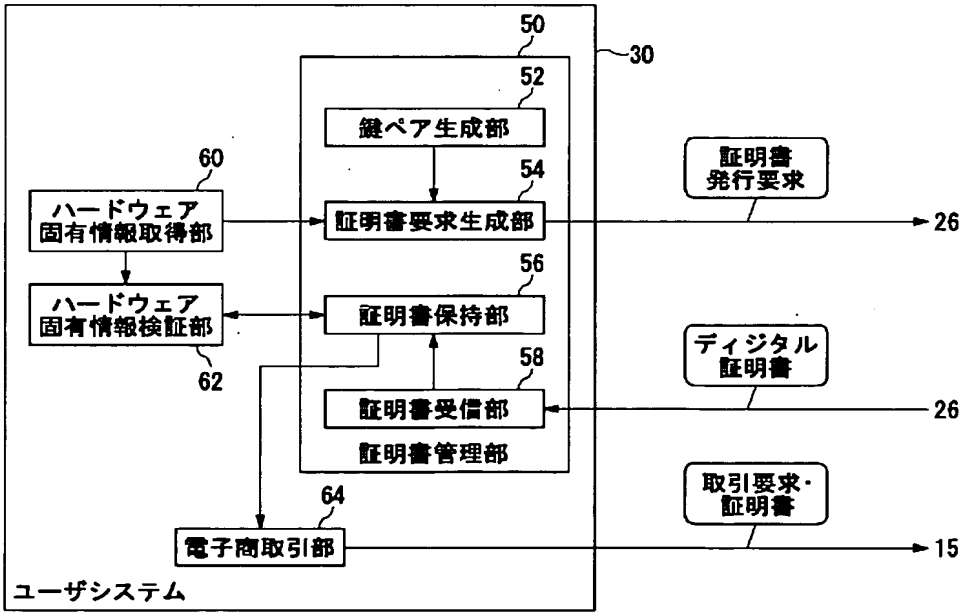
【図６】


12
14
10
Webサーバ
データベースサーバ
15
ショップシステム
オンラインショッピングサイト
16
メールサーバ
DNSサーバ
プロキシサーバ
認証装置
18
20
22
24
26
インターネットサービスプロバイダ
ユーザシステム
28
30
ユーザ端末

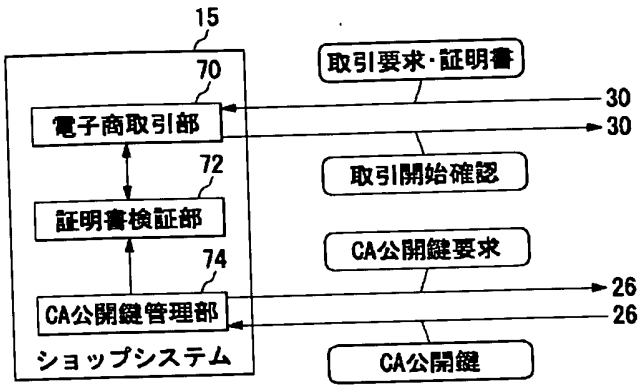
【図１０】


証明書の生成・発行
ユーザから
ハードウェア固有情報を含む
証明書発行要求を受信
S10
証明書データをハッシュ関数に
通してダイジェストを取る
S12
CAの秘密鍵でダイジェストを
暗号化し、電子署名を行う
S14
ユーザへ証明書を発行
S16
終了

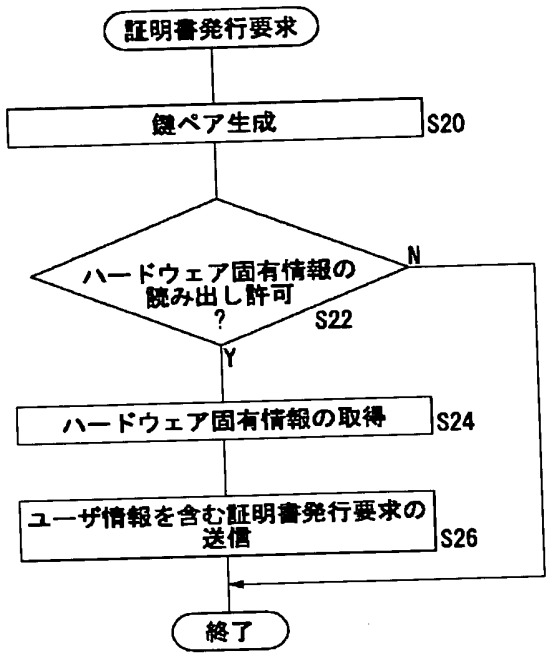
【図８】


50
30
52
鍵ペア生成部
60
54
ハードウェア固有情報取得部
証明書要求生成部
証明書発行要求
26
56
ハードウェア固有情報検証部
証明書保持部
62
58
ディジタル証明書
証明書受信部
26
証明書管理部
64
取引要求・証明書
電子商取引部
15
ユーザシステム

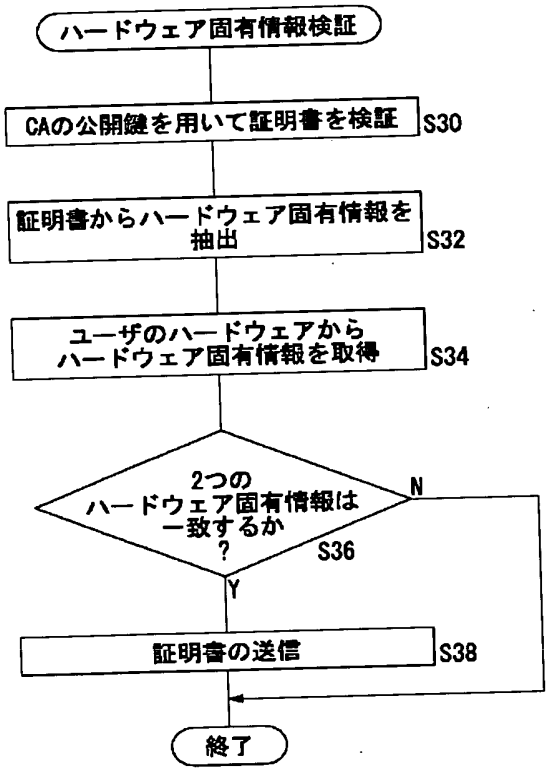
【図９】



【図１１】



【図１２】



【図１３】